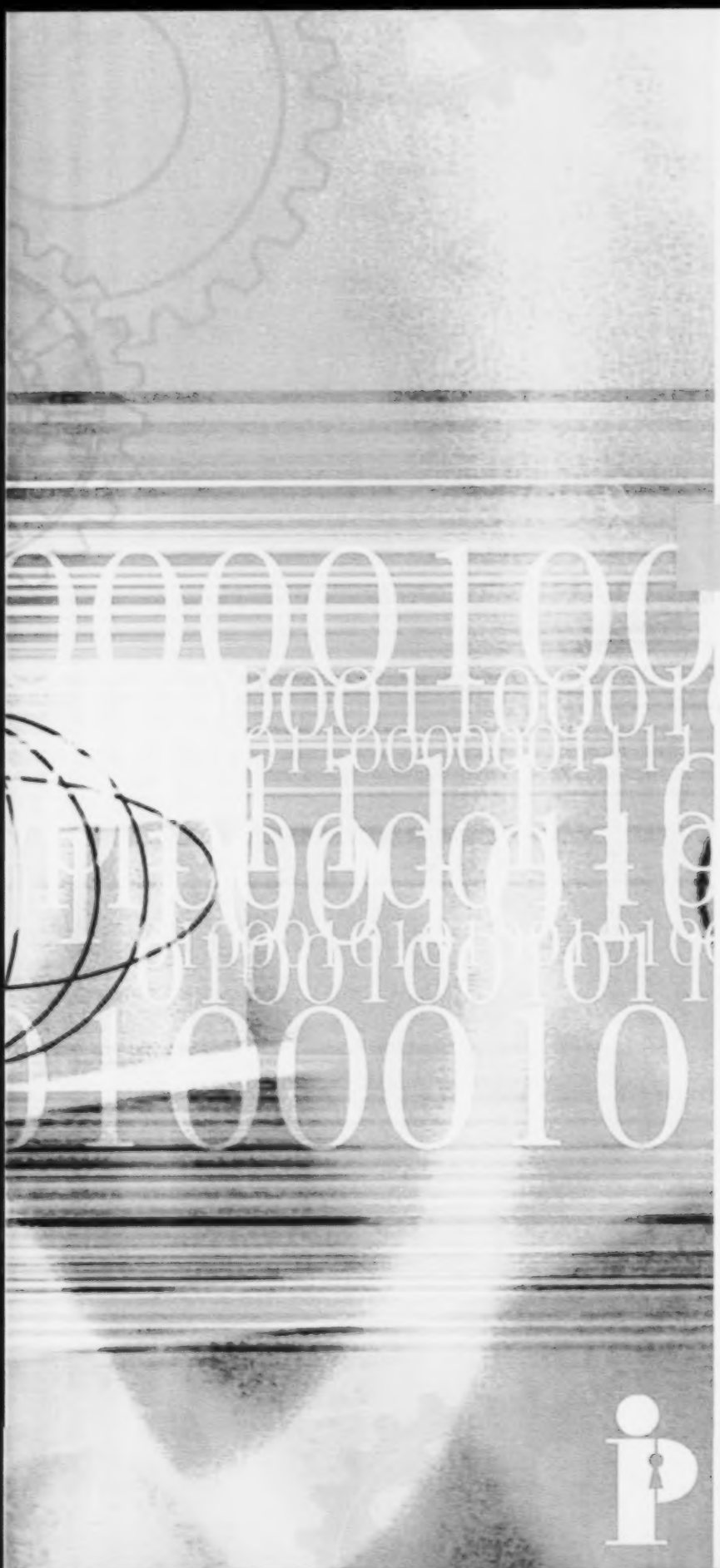


Be Proactive

... Avoid the Harm

INFORMATION & PRIVACY
COMMISSIONER OF ONTARIO
2010 ANNUAL REPORT

Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

May 17, 2011

The Honourable Steve Peters
Speaker of the Legislative Assembly

I have the honour to present the 2010 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1, 2010 to December 31, 2010.

Please note that additional reporting from 2010, including the full array of statistics, analysis and supporting documents, may be found within our online Annual Report section at www.ipc.on.ca

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosure

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

Commissioner's Message

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner,
Ontario, Canada

> I take my responsibility to protect the privacy of Ontarians very seriously, no matter where their personal information may actually reside — be it in Ontario, or in the Cloud!
>
> Commissioner Cavoukian

I carry out my mandate as Commissioner with three key words in mind — Consultation, Collaboration, and Co-operation. In 2010, that approach paid off handsomely with dozens of organizations and individuals, from every corner of the globe, reaching out to my office with a keen interest in taking their organizations, businesses and institutions forward into the 21st century, with regards to their privacy and access practices.

My message to all of them: Take charge! Be proactive, before the harm has arisen.

Taking a proactive approach lies at the heart of *Privacy by Design* (*PbD*) – embedding privacy directly into the design of technologies, business practices, and networked infrastructures. It makes privacy a foundational requirement, anticipating and preventing privacy-invasive events before they happen.

Similarly, it is central to my approach to freedom of information, which I have come to call *Access by Design* (*AbD*).

By embracing *AbD*, public organizations can improve their information management practices while at the same time, reducing the resource demands associated with relatively inefficient "reactive" disclosures.

In 2010, several institutions stood out in their commitment to being proactive about privacy and access. Hydro One, Toronto Hydro, and the Ontario Lottery and Gaming Corporation deserve special mention on the privacy front. In addition the Cities of Toronto and Ottawa earned special recognition, too, for their leading open data initiatives. Next year, I look forward to being able to report on even more leadership in these areas.

Privacy by Design: The New Gold Standard in Global Privacy

In my 2009 Annual Report, I wrote that, "PbD *is now a tangible and functioning reality and 2010 is already shaping up to be an even more promising year.*" As it turns out, these were prescient words! I could not have imagined the tipping point that this made-in-Ontario solution would reach in 2010.

This was apparent on many fronts, but perhaps the most exciting inroads made by *Privacy by Design* were on the international stage. It began early in the year, with Peter Hustinx, Europe's Data Protection Supervisor, recommending that *PbD* be included as a binding principle in the legal framework that is part of the European Commission's new European Digital Agenda. That seemed to set things in motion, as an avalanche of recognition ensued on its heels.

Springer's online journal, *Identity in the Information Society,* published a special *Privacy by Design Issue* in August that captured the proceedings of the "Definitive Workshop on *Privacy by Design*" that I hosted in Madrid, Spain. The Workshop brought together academic and business leaders to discuss how the next set of threats to privacy could best be addressed.

Premier Dalton McGuinty made a special address at the Commissioner's 2010 *Privacy by Design* Challenge event.

In early autumn, I attended the annual Conference of International Data Protection and Privacy Commissioners in Jerusalem, where I introduced a Resolution proposing that *PbD* be recognized as an essential component of fundamental privacy protection. The Resolution was unanimously passed by the entire assembly of Privacy Regulators from all around the world — transforming it overnight into a global standard. This was a real milestone for *PbD*, making it an international privacy standard — the gold standard!

A short while later, the Federal Trade Commission in the U.S. released a consultation document on its proposed policy framework, *Protecting Consumer Privacy in an Era of Rapid Change*, which recommended that companies adopt a *Privacy by Design* approach by building privacy protections directly into their everyday business practices.

As technologies such as cloud computing make borders increasingly irrelevant, it transforms the way in which we protect the privacy of those within our jurisdiction. As Commissioner, I take my responsibility to protect the privacy of Ontarians very seriously, no matter where their personal information may actually reside — be it in Ontario, or in the Cloud! Support for and implementation of *PbD* — a made-in-Ontario solution that we can all be proud of — continues to spread around the world. I am honoured that *PbD* has become part of the international privacy lexicon, and anticipate that these developments mark the beginning of what I believe will be the *Decade of Privacy by Design.* Stay tuned!

Privacy by Design in Action

Smart Grid

Ontario's Smart Grid program has proven to be very fertile ground for the application

Assistant Commissioner (Privacy) Ken Anderson addresses the crowd at the 2010 *Privacy by Design* Challenge.

and operationalization of *PbD*. At the heart of the Smart Grid will be a communications technology infrastructure that can collect and collate consumer data into useful and actionable information for both consumers and utilities. Left unchecked, however, the Smart Grid has the potential to erode privacy, collecting far more granular data about electricity consumption inside households than ever before.

This is why I have worked closely with electrical utility providers Hydro One and Toronto Hydro to embed privacy into Ontario's emerging Smart Grid. Working together in 2010, we produced a white paper, entitled *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*. This paper showed how the principles of *PbD* could be incorporated into the Smart Grid, and provided use-case scenarios related to customer information access and customer enablement.

Embedding privacy at the earliest stages will help to build consumer confidence and trust in the Smart Grid, allowing its benefits to be fully realized. I am deeply grateful to Hydro One and Toronto Hydro for collaborating with my office to set the standard for utilities across North America and around the world.

Biometric Encryption

Another breakthrough in 2010 was the application of the *PbD* principles to Biometric Encryption in the field of facial recognition technology.

In November, my office released a white paper, *Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept*, with the Ontario Lottery and Gaming Corporation (OLG). The paper announced a new facial recognition system that will check the faces of patrons entering gaming sites against a database of self-identified problem gamblers who have enrolled in a completely voluntary self-exclusion program. The system was developed in collaboration with iView Systems and University of Toronto researchers Professor Kostas Plataniotis and Dr. Karl Martin.

By applying the principles of *Privacy by Design*, and using a made-in-Ontario biometric encryption algorithm, the team of collaborators was able to embed a series of privacy-enhancing features. The new system does not store any data on non-enrolled patrons, while strongly protecting the privacy of enrollees by keeping data about them "locked" unless the person's live facial biometric appears. No single key can unlock the complete database of enrolled persons. A matching face will "unlock" only an enrollee's record, which will then be flagged for security staff to confirm it visually, and then escort the person off the premises consistent with their wishes.

Thousands of Ontarians have enrolled in the voluntary self-exclusion program, making manual enforcement increasingly difficult to sustain. This new, privacy-enhanced technology will enable the OLG to better support those who have enrolled in the program and offer dramatically improved privacy protection over simple facial recognition, without compromising any functionality, security or performance – the hallmarks of a *PbD* application.

Privacy by Design Curriculum

In 2010 we also released a new *Privacy by Design Curriculum* that will assist organizations that want to implement *PbD*. This resource is designed to equip chief

privacy officers, engineering instructors and social scientists to understand and teach others about *PbD*. The kit includes everything necessary to introduce basic privacy concepts and demonstrate how *PbD* may be applied in particular settings. Find the Curriculum, and much more, at www.privacybydesign.ca.

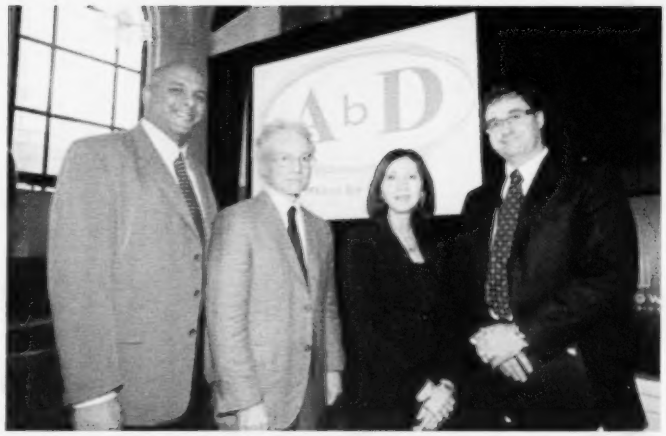
Access by Design

For the last two decades, the IPC has been at the forefront of campaigning for open, transparent, accountable government. In the past, our focus was on promoting *Routine Disclosure*. Advances in information and communications technology, however, have surpassed this concept, ushering in an era where *Proactive Disclosure* will become the norm.

Access by Design (*AbD*) addresses a fundamental change in the way that government and citizens interact, making public institutions proactive, rather than reactive, in their approach to disclosure. In short, *AbD* requires governments to recognize that publicly-held information is a public good, and that access should be provided *by default* – as part of an automatic process.

The concept of *AbD* goes much further, however. It also calls for a more responsive and efficient government that forges collaborative relationships with citizens, the private sector, and other public institutions. The ubiquitous nature of the Web, and accompanying technologies, has driven dramatic new increases in public demand for government-held information, giving a new dimension to civic participation and allowing for greater citizen engagement in policy making and service delivery.

I had the pleasure of hearing some wonderful *AbD* success stories in 2010 at our fifth annual *Right to Know* event, where representatives from Ontario's Ministry of the Environment and the City of Toronto shared details of their proactive disclosure programs. You can learn more about these and other examples, and the *7 Fundamental Principles of Access by Design*, in the *AbD* section of www.ipc.on.ca



(L-R) Steven Carrasco (Ministry of the Environment), Assistant Commissioner (Access) Brian Beamish, Commissioner Cavoukian and Dave Wallace (City of Toronto) at the IPC's 2010 Right to Know event.

My Personal Thank You

Each year, it seems that the demands on my office expand and grow. And each year, we rise to meet those demands. None of this would be possible without the hard work and dedication of my excellent staff. They rise to meet each and every new challenge with outstanding professionalism, and for that I am deeply grateful. Their commitment has made us a world-class agency, and a source of pride for me, personally, and for all Ontarians. You have my utmost thanks and appreciation!

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner, Ontario, Canada

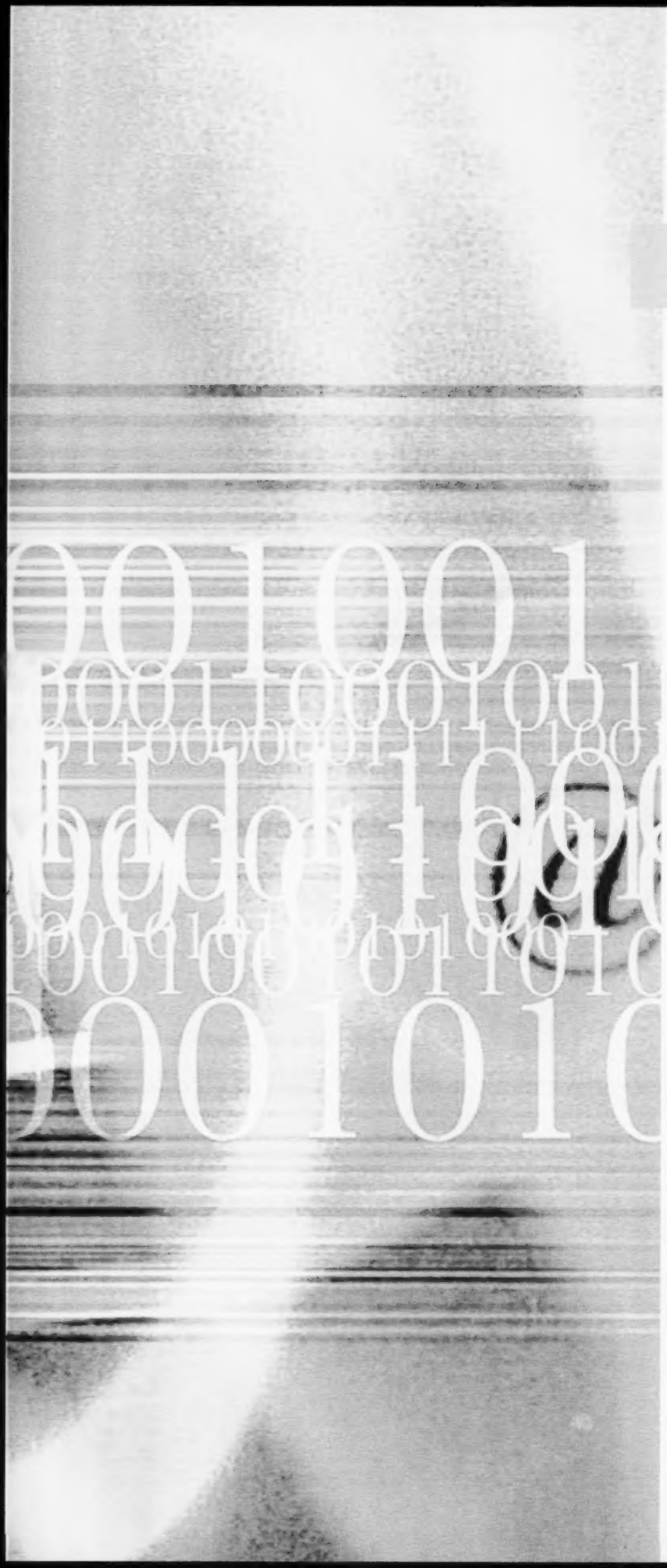


Table of Contents

Letter to the Speaker INSIDE FRONT

Commissioner's Message 1

A Call to Action 6

Key Issues 7

- Protecting Personal Health Information on Mobile Devices 7
- *Privacy by Design* Fostering Creativity and Innovation 7
- Rolling Back the Cost of Obtaining Our Health Records 7
- Opening the Door: Freedom of Information at Ontario Hospitals 9

Requests by the Public 10

Response Rate Compliance 11

FOI Appeals 12

Privacy Complaints 13

The *Personal Health Information Protection Act* (PHIPA) 14

Judicial Reviews 16

Financial Statement INSIDE BACK

Find more resources and full statistics in our online 2010 Annual Report section at www.ipc.on.ca.

A Call to Action

Become a *Privacy by Design Ambassador*

Here's your opportunity to join the frontline of a movement that is changing the way the world looks at privacy protection. *Privacy by Design* was never intended to serve as a conceptual abstraction – it can and must make real changes in our everyday lives.

I look forward to the day when building privacy into technology and business practices is considered to be second-nature, not a matter of debate. However, this will not be possible without your support. Together, we can assure a future that includes privacy:

1. Within your organization, identify an emerging technology or business practice that intersects with personally identifiable information and work towards building in the 7 Foundational Principles of *Privacy by Design*.
2. Share your ideas and insights with others on the *PbD* Global Forum.
3. Spread the word! Don't keep it to yourself – Use the *Privacy by Design* Curriculum to inform others about the benefits of *PbD*.

Find everything you need at www.privacybydesign.ca.

Become an *Access by Design Champion*

Government transparency and access to information are vital ingredients for a healthy and functioning democratic society. The concept of *Access by Design* consists of *7 Fundamental Principles* that I have developed to encourage public institutions to take a proactive approach to releasing information – access by default.

However, fostering this culture of accountability requires your participation:

1. Within your organization, identify information that could be made easier for citizens to access, and work towards building a proactive disclosure program.
2. Share your ideas and initiatives — send an email to abd@ipc.on.ca and we will profile your examples on our "AbD in Action" web page.
3. Spread the word! Inform others about the benefits of *AbD* – and introduce them to the *7 Fundamental Principles of Access by Design*.

To learn more, visit the *Access by Design* section at www.ipc.on.ca.

Protecting Personal Health Information on Mobile Devices

Over the past several years, the personal health information of hundreds of thousands of patients in Ontario has been compromised through the loss or theft of mobile devices. And while my office has issued three health orders — including HO-007, *Encrypt your Mobile Devices: Do it* ***Now***, in January of 2010 — along with several other publications on protecting personal information on mobile devices, it seems that our message has not sunk in with all levels of the health sector.

That is why in 2010, after yet another case of a USB key with unencrypted personal health information being stolen, we launched a proactive, multi-level education campaign called *"Stop. Think. Protect."* The campaign's focus is on building awareness among front-line health professionals that personal health information must never be stored on mobile devices such as laptops, PDAs and USB keys, unless it is absolutely necessary. And when it is, the data must be encrypted — Full Stop.

We wrote to regulatory health colleges and professional associations in Ontario, urging them to take part and offering our assistance in developing targeted educational materials for their members. We received outstanding support from the likes of the Ontario Dental Association, the College of Nurses of Ontario, the College of Dieticians of Ontario, Niagara Health System and many others.

Over the course of the campaign, we produced a series of articles, blogs, fact sheets, stickers, and other materials that were distributed throughout the system. We will be continuing this work into 2011.

The IPC launched an awareness campaign regarding personal health information on mobile devices.

Privacy by Design Fostering Creativity and Innovation

I have been a vocal proponent of *Privacy by Design* (*PbD*) – the concept of engineering privacy directly into the design of new technologies, business processes, and networked infrastructure as a core functionality — for many years. In 2010, that advocacy paid off as tremendous strides were made in evolving *PbD* from a conceptual framework into a practical one.

Several important *PbD* implementation projects came to fruition. *PbD* has been at the heart of ground-breaking work on the Smart Grid, and on the application of Biometric Encryption technology by the Ontario Lottery and Gaming Corporation (OLG) (*see the Commissioner's Message for details*).

We also saw significant privacy gains through the application of *Privacy by Design* in other arenas. Near the end of 2009, for example, my office worked closely with Google to develop a tip sheet on encrypting Gmail messages. Through that process, Google decided, in early 2010, to set the default so that it automatically encrypts, by default, all email messages sent by users of its Gmail service — a significant gain!

PbD also featured in the hot-button area of online targeted advertising. On television, everyone watching a particular program or broadcast feed sees the same ads. But on the web, advertisers can target specific ads to specific visitors. In order to do that effectively, of course, they benefit from knowing something about that person.

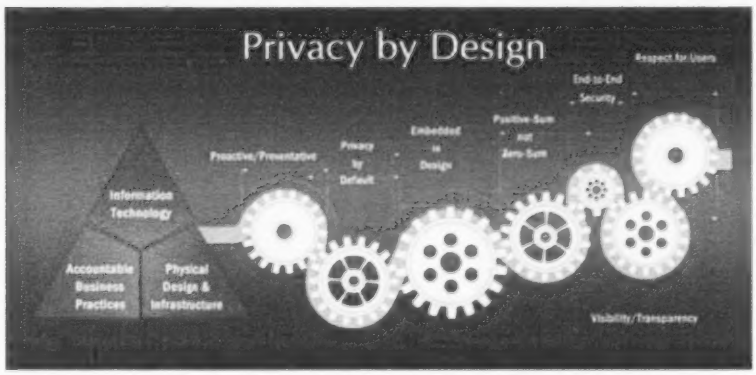
How much advertisers know about web users depends on the approach they take. "Behavioural" targeting, for example, aggregates users' actions into profiles, and delivers ads based on stated or inferred interests.

An increasingly popular approach is geographic (or geo-) targeting. "Geo targeting" is based on the identification of the real-world geographical location (geolocation) of an Internet-connected

device to deliver location-based advertising online.

In October 2010, we issued a white paper that examined the application of *Privacy by Design's* positive-sum paradigm to precise IP geolocation, working with Toronto's Bering Media, Inc. The company identified privacy issues inherent with the current implementations of geo-targeting, and redesigned the technique to improve functionality while greatly enhancing privacy. Our paper described Bering Media's innovative technology, which allows ISPs to partner with an ad server to provide IP geolocation services without *any* disclosure of personally identifiable information about subscribers. Using this innovative technology, the ISP can partner with an ad server without the server reading or modifying any packets travelling through the ISP's network.

Bering Media has truly embraced the spirit of *Privacy by Design*, demonstrating a technology that functions in a positive-sum manner by allowing online targeting through IP geolocation to be implemented in a privacy-protective manner. Like our other *PbD* projects this year, Bering Media demonstrated the extent to which innovation is fostered when you abandon the widespread, but misguided view, that privacy and other objectives are necessarily in conflict.



Learn more about the Commissioner's core concept of *Privacy by Design* at www.privacybydesign.ca.

Rolling Back the Cost of Obtaining Our Health Records

Health Order HO-009 has implications for Ontarians seeking to access their own health records.

Since the *Personal Health Information Protection Act* (*PHIPA*) came into force in 2004, we have urged the provincial government to bring in a regulation to prescribe specific fees that health information custodians may charge individuals to access copies of their own personal health information records. In the absence of a prescribed amount, *PHIPA* permits custodians to charge the amount of "reasonable cost recovery."

The right of access to one's own records of personal information is a cornerstone of fair information practices and privacy legislation. In the context of health care, the right of access enables individuals to determine what shall or shall not be done with their own bodies, to exercise control over the collection, use or disclosure of their own personal health information, and to require the correction or amendment of their information. It is also vital to ensuring continuity of care. Any interpretation of the term "reasonable cost recovery" that imposes a financial barrier or deters individuals from exercising their right of access to records must be avoided.

In March 2006, the Minister of Health and Long-Term Care published a draft regulation prescribing the fees that a health information custodian may charge for access. To date, however, no such

regulation has been passed, leaving the fee required to the discretion of custodians. With widespread discrepancies across the health sector, some custodians charge excessive fees that pose barriers to access, resulting in complaints to the IPC.

In 2010, the Assistant Commissioner (Access) issued Order HO-009 after a patient complained about the $125 fee charged by her physician for access to 34 pages of her records. After reviewing a number of fee schemes, including the regulations made under the provincial and municipal *Freedom of Information and Protection of Privacy Acts*, the Ontario Medical Association *Guide*, and the discretionary flat fee recommended by the Ontario Hospital Association, Assistant Commissioner Beamish determined that the fee scheme set out in the proposed regulation published in 2006, provided the best framework for determining the amount of "reasonable cost recovery."

The Assistant Commissioner found that the $125 fee exceeded "reasonable cost recovery" under *PHIPA*. Based on applicable calculations, the physician was ordered to reduce the fee to $33.50.

Until a regulation governing fees is introduced, the IPC — when dealing with complaints regarding fees charged for providing copies of a patient's personal health information — will continue to use the proposed 2006 regulation as a guideline.

Opening the Door: Freedom of Information at Ontario Hospitals

Transparency and accountability in Ontario hospitals took a major leap forward in 2010 with the passage of the *Broader Public Sector Accountability Act*, which brings hospitals under Ontario's *Freedom of Information and Protection of Privacy Act* (*FIPPA*).

Since 2004, hospitals have been covered under the *Personal Health Information Protection Act* (*PHIPA*), which governs the collection, use and disclosure of personal health information by the health sector.

Ontario Hospitals are to be covered by Freedom of Information legislation for the first time.

Now, bringing hospitals under the province's FOI legislation completes the circle, providing a wide right of access to records under a hospital's custody or control relating to administrative and operational functions, financial considerations and decisions, and personal information.

Freedom of information legislation will apply to hospitals as of January 1, 2012. After that date, citizens will have the right to make a request for access to a range of recorded information that came into the custody or under the control of a hospital on or after January 1, 2007.

Ontario was the last province to bring hospitals under FOI legislation. I am delighted that the government has finally moved forward with this important step, and recognized that in a free and democratic society, people have a right to hold institutions, that are funded by public dollars, accountable.

For more information on all of these key issues, visit www.ipc.on.ca.

Requests by the Public

2010 FOI Requests, by Jurisdiction and Records Type

	Personal Information	General Records	Total
Municipal	11,515	12,227	23,742
Provincial	4,319	10,842	15,161
Total	**15,834**	**23,069**	**38,903**

A record number of freedom of information (FOI) requests were filed across Ontario in 2010. A total of 38,903 requests were filed in 2010, eclipsing the previous record of 38,584, set in 2007. The spike in 2010 represented the first increase in FOI requests in three years.

Provincial government organizations received 15,161 FOI requests in 2010, an increase of more than 8.1 per cent from 14,023 in 2009. Of the requests filed, 4,319 (28.4 per cent) were for records containing the personal information of the requestor, while 10,842 (71.5 per cent) were for general records.

The Ministry of the Environment continued to receive the largest number of requests under the provincial *Act* — 5,531 in 2010, an increase of 587 requests from 2009. In a repeat of 2009, the other ministries at the top of the heap in terms of requests received were Community Safety and Correctional Services with 4,271, Community and Social Services at 785, and Labour with 742 requests (the largest annual increase of the four ministries at 20.5 per cent). Combined, these four ministries continued to receive the vast majority of requests with three-quarters (75 per cent) of all provincial requests in 2010.

Municipal government organizations received 23,742 FOI requests in 2010, a marginal increase of 2.9 per cent from the 23,067 requests in 2009. While FOI requests to the City of Toronto have continued to drop significantly, the remaining municipal requests have continued to increase, climbing from 19, 887 in 2008 to 21, 593 in 2010. Of the FOI requests made to municipal institutions in 2010, 11,515 (48.5 per cent) were for personal information and 12,227 (51.5 per cent) were for general records.

The significant drop in the number of FOI requests to the City of Toronto may be attributed to the continued success of its routine disclosure program (www.toronto.ca/cap/disclosure.htm) as well as other proactive disclosure measures introduced (see our *"Access by Design"* section at www.ipc.on.ca to learn more). Significant progress has been made in diverting traditional FOI requests, with the City of Toronto receiving 2,129 requests in 2010 – less than half of the 4,595 requests it received in 2008.

Of the top ten municipal institutions to receive FOI requests, half were to police services boards, which continued to receive by far the most requests under the municipal *Act* — 13,061 (55.0 per cent). Municipal corporations were next with 9,648 requests, followed by school boards with 242 requests and health boards with 83 requests.

Continuing a positive trend, the average fees charged in 2010 for general records by provincial institutions remained steady at just under $40 – down from over $51 in 2006.

See full statistics related to 2010 FOI requests at www.ipc.on.ca

Average Cost of Provincial Requests

	2006	2007	2008	2009	2010
Personal Information	$11.55	$10.54	$11.26	$ 9.47	**$12.88**
General Records	$51.11	$50.54	$42.74	$39.66	**$39.97**

Average Cost of Municipal Requests

	2006	2007	2008	2009	2010
Personal Information	$ 8.64	$ 9.67	$ 8.82	$ 8.11	**$8.01**
General Records	$21.04	$23.49	$23.54	$26.55	**$25.68**

Response Rate Compliance

Top 10 Provincial Institutions: Ranked by the number of requests completed in 2010

	Requests Received	Requests Completed	Within 30 Days	%	Extended Compliance *	Over 90 Days	%
Ministry of the Environment	5,531	5,364	4,503	83.9	85.4%	158	2.9
Ministry of Community Safety & Correctional Services	4,271	4,231	3,760	88.9	95.4%	136	3.2
Ministry of Community & Social Services	785	861	655	76.1	76.5%	28	3.3
Ministry of Labour	742	723	663	91.7	100.0%	1	0.1
Ministry of the Attorney General	433	388	352	90.7	95.6%	1	0.3
Archives of Ontario	374	362	327	90.3	99.4%	3	0.8
Liquor Control Board of Ontario	345	347	334	96.3	96.5%	0	0.0
Ministry of Transportation	356	334	302	90.4	93.1%	6	1.8
Landlord and Tenant Board	269	236	232	98.3	98.3%	0	0.0
Ministry of Health and Long-Term Care	218	217	92	42.4	65.9%	63	29.0

*Including Notice of Extension, section 27(1) and Notice to Affected Persons, section 28(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.

The IPC reports compliance rates to help focus attention on the importance for government organizations to comply with FOI response requirements set out in the *Acts* (although, timeliness alone does not provide a full indication of the quality of FOI responses). The provincial 30-day compliance rate has continued to climb from 42 per cent to over 80 per cent since the IPC first reported individual response rates in 1999.

Institutions Governed Under the Provincial *Act*

Provincial ministries, agencies and other institutions regained ground in 2010, achieving an overall 30-day compliance rate of 84.7 per cent. This was up from 81 per cent in 2009, but just below the high of 85 per cent in 2008. The majority of requests completed by provincial organizations came from the business sector at 9,688 (65.2 per cent) followed by requests from individuals at 3,703 or 24.9 per cent.

After setting a record in 2009 at 97.2 per cent, 2010's provincial extended compliance rate fell back to 90.1 per cent. (Extended compliance rates — where institutions can respond later than 30 days because of qualified extenuating circumstances — have only been calculated since 2002.)

The Ministry of Health and Long-Term Care saw its extended compliance rate drop from 86.2 per cent in 2009 to 65.9 per cent in 2010. However, the Ministry notes that 25 per cent of its *FIPPA* files for 2010 were carried over from 2009. When only requests received in 2010 are considered, the Ministry achieved an overall compliance rate of 86 per cent. The Ministry also notes a significant increase in the number of requests that can be considered complex and that require greater processing time. The Ministry has implemented several strategies in 2010 to improve the overall performance of its Access and Privacy Office.

The Ministry of Community Safety and Correctional Services saw a significant increase in its 30-day compliance rate from 76.2 per cent in 2009 to 88.9 per cent in 2010.

Institutions Governed by the Municipal *Act*

Municipal government organizations matched their provincial counterparts in responding to FOI requests within the statutory 30-day period, coming in at 85.4 per cent. With extension notices, the municipal response rate rises to 88.4 per cent. Requests from individuals made up the majority of requests completed by municipal organizations at 16,283 (70.1 per cent) followed by the business sector at 5,561 or 23.9 per cent.

Continuing a trend from 2009, Toronto Police Services has replaced the City of Toronto as the municipal institution that completed the most FOI requests at 4,324 with a 30-day compliance rate of 77.5 per cent (81.3 per cent extended). The City of Toronto, which completed 2,065 requests, had a 30-day 83.3 per cent compliance rate (84.9 per cent extended), followed by Peel Regional Police, which completed 1,643 requests and continued to uphold their outstanding 100 per cent completion record for both 30-day compliance and extended compliance rate.

See complete 2010 response rates for ministries, municipalities, police forces, school boards, etc. at www.ipc.on.ca.

FOI Appeals

Summary of Appeals: 2010 vs. 2009

2010	General Records			Personal Information			Total		
	Provincial	Municipal	Total	Provincial	Municipal	Total	Provincial	Municipal	Total
Opened	328	306	634	121	222	343	449	528	977
Closed	257	302	559	139	218	357	396	520	916

2009	General Records			Personal Information			Total		
	Provincial	Municipal	Total	Provincial	Municipal	Total	Provincial	Municipal	Total
Opened	367	280	647	164	189	353	531	469	1,000
Closed	385	302	687	151	178	329	536	480	1,016

If you make a written freedom of information (FOI) request under Ontario's provincial or municipal *Freedom of Information and Protection of Privacy Acts*, and are not satisfied with the response, you have a right to appeal that decision to the IPC. Appeals may relate to a refusal to provide access, fees sought, the fact that the institution did not respond within the prescribed 30-day period, refusal to correct your personal information, or other procedural aspects relating to a request.

2010 Appeals

In 2010, 977 appeals were **submitted** to the IPC – the second highest number in 15 years, trailing only 2009's 1,000 appeals. Overall, 916 appeals were **closed** in 2010, slightly above the average for the past decade.

Records that do not contain the personal information of the requester are referred to as *general records*. Overall, 634 appeals regarding access to *general records* were made to the IPC in 2010. Of these, 328 were filed under the provincial *Act* and 306 under the municipal *Act*.

There were a further 343 *personal information* appeals filed to the IPC in 2010, including 121 under the provincial *Act* and 222 under the municipal *Act*.

In 2010, the number of appeals opened under the municipal *Act* – 528 – was up by 59, while the number filed under the provincial *Act* – 449 – was down 82 from the previous year.

Of the 449 appeals filed with the IPC under the provincial *Act*, 105 (23 per cent) involved the Ministry of Health and Long-Term Care, while another 101 (22.5 per cent) involved the Ministry of Community Safety and Correctional Services. A further 20 appeals related to decisions of the Ministry of the Attorney General, followed by the Ontario Power Authority (15), and the Ministries of Environment (14) and Government Services (12). The University of Ottawa again had more appeals filed against its decisions than any other university, although the number dropped to 12 in 2010 from 29 in 2009.

Of the 528 appeals the IPC received under the municipal *Act*, 227 (43 per cent) involved police services, while 217 (41 per cent) involved municipalities. Toronto Police Services, which received more requests under the municipal *Act* than any other government organization, was also involved in the most appeals under that *Act* (77), followed by the City of Toronto (43), Peel Police Services (26), Halton Police Services (26), Ottawa Police Services (18) and the cities of Ottawa and Greater Sudbury, both with 12.

The Thames Valley District School Board was involved in the most appeals against a school board (seven), followed by the Algonquin and Lakeshore Catholic District School Board (six). Algoma Public Health was the health unit involved in the most appeals (six).

For more detailed information about appeals filed and closed in 2010, see the statistical adjunct of this annual report, available at www.ipc.on.ca.

Summary of Privacy Complaints: 2010 vs. 2009

	2009 Privacy Complaints				2010 Privacy Complaints			
	Provincial	Municipal	Non-jurisdictional	Total	Provincial	Municipal	Non-jurisdictional	Total
Opened	120	144	0	**264**	127	125	0	**252**
Closed	101	126	0	**227**	130	137	0	**267**

Ontario's provincial and municipal *Freedom of Information and Protection of Privacy Acts* establish rules that govern the collection, retention, use, disclosure, security, and disposal of personal information held by government organizations.

If you believe that your privacy has been compromised by a provincial or local government organization, you can file a complaint under the *Acts* with the IPC. In the majority of cases, the IPC attempts to mediate a solution. The IPC may also make formal recommendations to a government organization to amend its practices.

Privacy Complaints

A record 267 privacy complaints were **closed** by the IPC in 2010, easily surpassing the 241 privacy complaints closed in 1996 – the previous record.

The 267 privacy complaints closed under the public sector *Acts* in 2010 included 137 under the municipal *Act* and 130 under the provincial *Act*. The IPC also closed 179 *collection, use* or *disclosure complaints* under the *Personal Health Information Protection Act (PHIPA)*, taking the total number of privacy complaints closed in 2010 to 446. This total was 45 (or just over 10 per cent) more than the previous year.

There were 252 privacy complaints **opened** under the two public sector *Acts* in 2010 – the second highest total since the first of these *Acts* – the *Freedom of Information and Protection of Privacy Act* – came into effect in 1988. The record – 264 – was set in 2009.

Of the 252 privacy complaints opened in 2010, 127 (just over 50 per cent) were filed under the provincial *Act* and 125 under the municipal *Act*. When the 188 *collection, use* or *disclosure privacy complaints* filed under Ontario's *PHIPA* are added, the total number of privacy complaints filed with the IPC in 2010 climbs to 440 – seven more than the previous year. (See page 14 for more detailed statistics related to *PHIPA*.)

As has been the case for years, the most cited reason for filing a privacy complaint under the two public sectors *Acts* was the disclosure of personal information. Disclosure was raised as an issue in 136 of the complaints closed (59.1 per cent). Another 31 (3.5 per cent) were related to security, while collection of personal information was an issue in 30 cases (13 per cent). The remaining complaints involved such issues as retention, use, notice of collection and disposal.

The IPC continues to emphasize informal resolution and 251 of the 267 privacy complaints were closed without the issuance of a formal privacy complaint report or order.

Of the complaints closed, 165 (about 62 per cent) had been initiated by individual members of the public, while 12 (4.5 per cent) were Commissioner-initiated. A further 90 (about 34 per cent) were self-reported breaches.

For more detailed information about privacy complaints in 2010, see the statistical adjunct of this annual report, available at www.ipc.on.ca.

The Personal Health Information Protection Act (*PHIPA*)

Summary of *PHIPA* Complaints: 2010 vs. 2009

	2009 *PHIPA* Complaints					2010 *PHIPA* Complaints				
		Collection/Use/Disclosure					Collection/Use/Disclosure			
	Access / Correction	Individual	Self-Reported Breach	IPC - initiated	Total	Access / Correction	Individual	Self-Reported Breach	IPC - initiated	Total
Opened	79	55	101	13	248	100	62	95	31	288
Closed	66	59	102	13	240	112	59	98	22	291

The number of complaints filed with the IPC under the *Personal Health Information Protection Act (PHIPA)* rose to 288 in 2010, an increase of 16 per cent from the 248 filed in 2009 – and the second highest total in the six full years since *PHIPA* came into effect.

Public hospitals were the subject of 97 of the 288 files opened, or about 34 per cent. Of these, 31 (32 per cent) were self-reported breaches related to the collection, use, or disclosure of personal health information. Commissioner Cavoukian actively encourages this kind of self-reporting by health information custodians and the IPC is committed to working with custodians to take quick steps to deal with breaches.

There were 52 complaints opened involving doctors — double the 26 filed in 2009 — 27 of which related to access to and/or correction of personal health information. The number of complaints opened involving clinics climbed to 30 from 17, an increase of over 76 per cent.

Complaints Closed

The increase in the number of complaint files opened was partially reflected in the number of complaints *closed*. The IPC closed 291 complaints in 2010, an increase of about 21 per cent over the 240 complaints closed in 2009. This rise in complaints closed was primarily triggered by an increase in the cases involving access to and/or correction of personal health information – from 66 in 2009 to 112 in 2010, an increase of almost 70 per cent. The remaining 179 complaints closed in 2010 dealt with the collection, use, or disclosure of personal health information. Of these, 98 were self-reported breaches; 59 were initiated by individuals; and 22 were IPC-initiated.

As much as possible, the IPC prefers to resolve complaints either informally or through mediation. Of the 112 complaints closed that were related to access to and/or correction of personal health information, 78 (nearly 70 per cent) were closed informally at the intake stage; 25 (about 22 per cent) were closed during the mediation stage; and nine (just over eight per cent) were closed during the adjudication stage, one of which resulted in the IPC issuing a health order (HO-009).

Of the 98 complaints that involved self-reported privacy breaches by health information custodians, 94 (almost 96 per cent) were closed at the intake stage, and two were closed with the IPC issuing health orders (HO-007, HO-008).

Applying *PHIPA* and *FIPPA/MFIPPA* to Personal Health Information

January 1, 2012 heralds a new era at Ontario hospitals as they become institutions under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). Commissioner Cavoukian has long advocated for this course of action to foster a culture of increased accountability at Ontario hospitals, and reinforce Ontarians' "right to know."

Since 2004, hospitals have been defined as health information custodians under *PHIPA*, which governs the collection, use and disclosure of personal health information by the health sector. *PHIPA* gives individuals the right, with limited exceptions, to access their own personal health information. With the introduction of *FIPPA*, the general public will have a broader right to access hospital records relating to administrative and operational functions; financial considerations and decisions; and personal information that came into the custody or under the control of hospitals on or after January 1, 2007.

IPC has issued a new fact sheet for all organizations that are defined as both health information custodians and institutions (covered by *PHIPA* as well as *FIPPA* or *MFIPPA*), specifically addressing the application of the statutes to personal health information. See **www.ipc.on.ca**.

Type of *PHIPA* Complaint Files Opened in 2010

			Collection/Use/Disclosure							
	Access/ Correction	%	Individual	%	Self-reported Breach	%	IPC-initiated	%	Total	%
Public Hospital	33	33.0	24	38.7	31	32.6	9	29.0	97	33.7
Doctor	27	27.0	7	11.3	8	8.4	10	32.3	52	18.1
Clinic	9	9.0	7	11.3	11	11.6	3	9.7	30	10.4
Community or Mental health centre, program or service	6	6.0	3	4.8	10	10.5	1	3.2	20	6.9
Community Care Access Centre	2	2.0	0	0.0	10	10.5	1	3.2	13	4.5
Ministry of Health and Long-Term Care	5	5.0	4	6.5	0	0.0	0	0.0	9	3.1
Other Health-Care professional	2	2.0	1	1.6	5	5.3	1	3.2	9	3.1
Dentist	3	3.0	2	3.2	2	2.1	1	3.2	8	2.8
Laboratory	0	0.0	3	4.8	4	4.2	0	0.0	7	2.4
Minister of Health and Long-Term Care	4	4.0	0	0.0	0	0.0	1	3.2	5	1.7
Other	1	1.0	3	4.8	1	1.1	0	0.0	5	1.7
Agent	0	0.0	1	1.6	2	2.1	0	0.0	3	1.0
Long-term care facility	1	1.0	1	1.6	1	1.1	0	0.0	3	1.0
Pharmacist	1	1.0	1	1.6	1	1.1	0	0.0	3	1.0
Physiotherapist	0	0.0	0	0.0	2	2.1	1	3.2	3	1.0
Psychiatric Facility	3	3.0	0	0.0	0	0.0	0	0.0	3	1.0
Ambulance services	0	0.0	0	0.0	1	1.1	1	3.2	2	0.7
Independent Health Facility	0	0.0	0	0.0	1	1.1	1	3.2	2	0.7
Institution - Mental Hospitals Act	0	0.0	1	1.6	1	1.1	0	0.0	2	0.7
Optometrist	1	1.0	1	1.6	0	0.0	0	0.0	2	0.7
Pharmacy	0	0.0	0	0.0	1	1.1	1	3.2	2	0.7
Other	2	2.0	3	4.8	3	3.3	0	0	8	2.4
Total	100		62		95		31		288	

Of the 59 complaints initiated by individuals related to the collection, use, or disclosure of personal health information, 58 (98 per cent) were closed during the intake stage, with one order issued during the adjudication stage (HO-010). Finally, of the 22 IPC-initiated complaints dealing with the collection, use, or disclosure of personal health information, 19 (just over 86 per cent) were closed at the intake stage.

Personal Health Information Requests

Only health information custodians who also fall under *FIPPA* or *MFIPPA* are required to report to the IPC the number of requests they receive from individuals seeking their own personal health information.

Custodians reported the completion of 5,044 such requests in 2010. The Ministry of Health and Long-Term Care completed 4,079 of these, almost 81 per cent. The requests made to the ministry climbed by 956 from 2009's 3,123 requests, an increase of nearly 31 per cent. The ministry was able to complete 4,069 requests, or 99.8 per cent, within the statutory 30-day compliance period.

See a full report of developments and statistics related to PHIPA in 2010 at www.ipc.on.ca.

Judicial Reviews

A number of significant Court decisions released in 2010 dealt with difficult issues involving the relationships between the statutory right of access, the *Charter of Rights and Freedoms* and the administration of criminal and civil justice, including issues of common law privilege.

Order PO-1779 – Ontario (Public Safety and Security) v. Criminal Lawyers' Association[1]

In 2010 the Supreme Court of Canada released its long-awaited decision in the Criminal Lawyers' Association (CLA) case dealing with the relationship between access rights under *FIPPA* and the freedom of expression under section 2(b) of the *Charter of Rights and Freedoms*.

The appeal arose out of a request by the CLA for access to a report and other records relating to the OPP's investigation into the conduct of Crown lawyers and police in a murder prosecution. The trial judge was highly critical of this conduct and stayed the charges against the accused. However, the OPP stated in a news release that it had found no evidence of misconduct.

The IPC held that the exemptions for law enforcement, solicitor-client privilege and personal privacy applied to the records. The IPC also found a compelling public interest in their disclosure which clearly outweighed any privacy interests pursuant to the override clause at section 23 of the *Act*. However, because the other two exemptions are not included in the public interest override and, further, because this exclusion did not impinge on the freedom of expression as the CLA had argued, the IPC upheld the Ministry's refusal to disclose all three records.

The Supreme Court of Canada affirmed the IPC's decision. While the Court recognized that access to information is a "derivative right" under section 2(b) "which may arise where it is a necessary precondition of meaningful expression on the functioning of government," it gave three reasons for holding that section 2(b) was not implicated in this case:

(1) the CLA was not precluded from expressing itself on a matter of public interest since the trial judge's ruling placed the essential allegations of misconduct on the public record;

(2) the CLA had not shown that access would not impinge on the government's interests protected by the exemptions; and

(3) the Ministry's statutory discretion to disclose the records already incorporates public interest considerations.

Aside from the *Charter* issue, the judgment is significant for affirming "reasonableness" as the standard for reviewing IPC decisions, and for articulating the broad scope of IPC's power to review the exercise of an institution's discretion to refuse disclosure.

See more information on this ruling, and additional key Court rulings in the 2010 Judicial Reviews report at www.ipc.on.ca

2010 Judicial Review Statistics

Judicial Reviews Closed/Heard in 2010	16
Abandoned (IPC Order/decision stands)[2]	6
Heard but Not Closed (decision pending)[3]	2
IPC Order Upheld[4]	2
IPC Order Partially Upheld[5]	1
IPC Order Not Upheld (motion for leave to appeal pending)[6]	1
IPC Order Not Upheld[7]	3
IPC Intervened in application[8]	1

1 2010 SCC 23

2 PO-2620 (2 JRs), PO-2263-I / PO-2286-I, Complaint HA09-60, Appeal PA09-330

3 PO-2739, MO-2425-I

4 MO-2294, MO-2481

5 PO-1779

6 MO-2408

7 Appeal PA08-92, PO-2405 / PO-2538-R

8 City of Toronto

Financial Statement

	2010-2011 Estimates $	2009-2010 Estimates $	2009-2010 Actual $
Salaries and Wages	9,461,000	9,414,000	9,214,586
Employee Benefits	2,176,200	2,165,200	1,662,165
Transportation and Communications	313,500	296,000	294,071
Services	1,890,800	1,812,300	1,895,502
Supplies and Equipment	194,000	194,000	483,998
Total	**14,035,500**	**13,881,500**	**13,550,322**

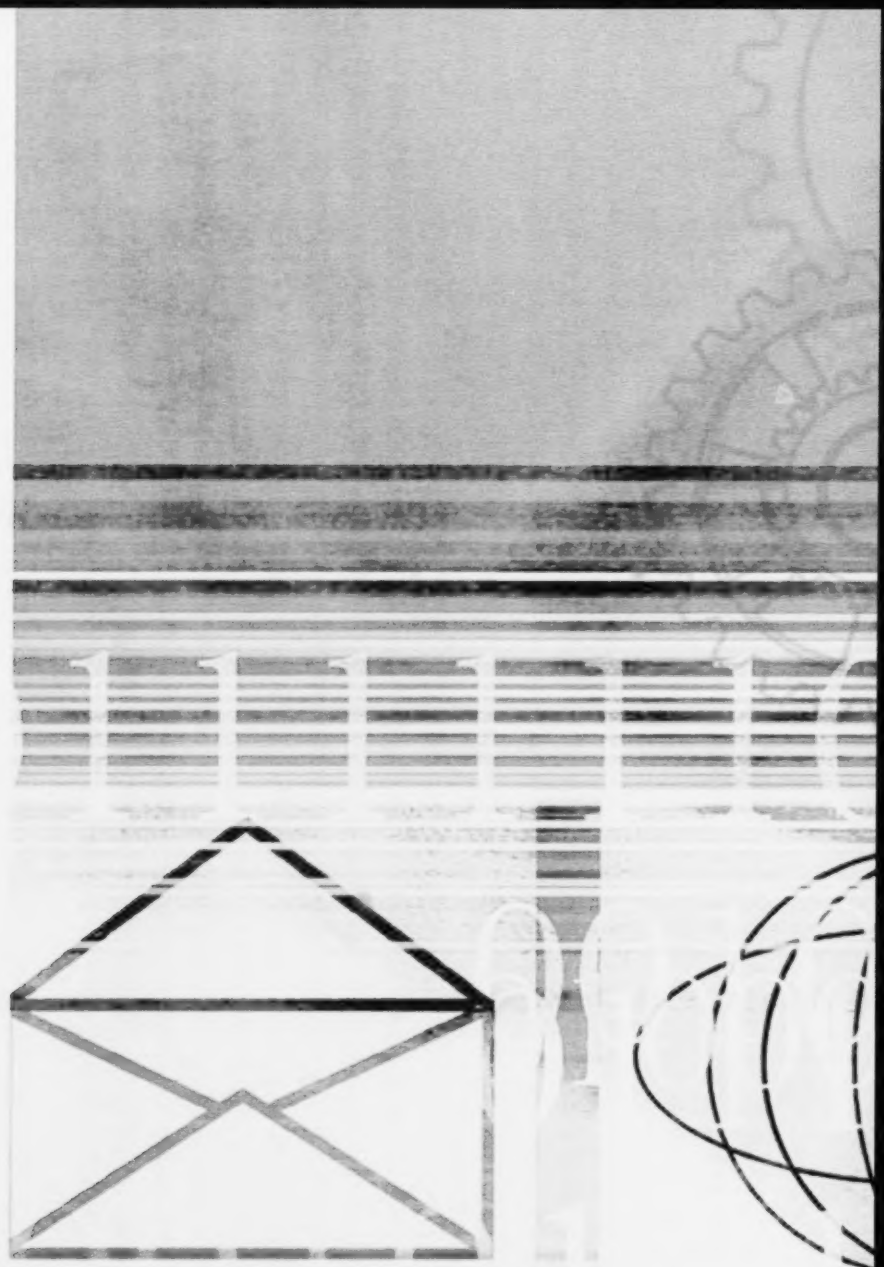
Note: The IPC's fiscal year begins April 1 and ends March 31.
The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

2009 Appeals Fees Deposit

(Calendar year)

General Info.	Personal Info.	Total
$9,615	$2,355	**$11,970**

See further financial information, including IPC Public Sector Salary Disclosure, at www.ipc.on.ca



INFORMATION & PRIVACY
COMMISSIONER OF ONTARIO
2010 ANNUAL REPORT

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada

Tel: (416) 326-3333
Fax: (416) 325-9195
1-800-387-0073
TTY: (416) 325-9539

E-mail: info@ipc.on.ca
Web: www.ipc.on.ca